Written by C. Mitchell Shaw on December 10, 2018

New Aussie Law Attacks Encryption, Threatens Privacy and Liberty

Australia has passed a controversial ant-encryption law that will allow law-enforcement and intelligence agencies to spy on the encrypted communications of individuals. The new law requires technology companies to create and deploy backdoor vulnerabilities on "one or more technologies that are connected with a particular person" — as long as that "particular person" is suspected of being a terrorist or criminal.

In reality, the new law threatens the privacy and liberty of all.

The passage of the law in the Australian Senate was a major surprise for those tracking the bill. The Labor Party had vowed to defeat the bill after it passed in the Senate. Without the support of Labor, the bill seemed destined for failure. Labor had said all along that the bill would not receive the needed votes without amendments to ameliorate the more onerous provisions in the legislation. But in the final hour, Labor decided to back the bill, allowing overwhelming passage of 44 votes to 12.

As IT News is reporting:

> It was only a last-minute offer — made through a press conference by Opposition Leader Bill Shorten and Shadow Attorney-General Mark Dreyfus on Thursday night — that cleared its path.
>
> Shorten said that Labor wanted to pass the encryption bill into law tonight "so we at least give our intelligence agencies some of the tools they need".
>
> "We offer to let the bill go forward, without the amendments which are needed … provided the government agrees on the very first sitting day, to pass the amendments we say are needed," Shorten said.
>
> "What we say to the government right now is if you agree to do the amendments that you've already agreed to do to the encryption laws in the first week of next year, we will pass the encryption laws — unsatisfactory as they are — right now.
>
> "I'm not willing to go home and see a terror event happen — which we're told is less likely than more likely — but I'm not going to have on my conscience [Prime Minister Scott] Morrison's hostage-taking tactics where he cancels his own work, goes home and lets Australians swing in the breeze."

There are multiple problems with Australia's new anti-encryption law — all of which will have a negative impact far beyond the Land Down Under.

First, while Aussie legislators — including Labor — claim that the bill is geared toward giving "intelligence agencies some of the tools they need," the reality is that laws designed to defeat encryption have almost nothing to do with combating terrorism. As Shorten even admitted, a terrorist

attack due to the presence of strong encryption "is less likely than more likely."

The reason for that is that encryption is simply a math equation. And while Australia's new law may force legitimate tech companies to weaken the encryption they offer to Aussies, nothing — absolutely nothing — prevents terrorist and criminal organizations from writing their own encryption algorithms. In fact, as multiple cases in the past have shown, that is exactly what many of them do.

So, what Australia's legislature passed is a law that creates backdoor vulnerabilities that could (and will) impact law-abiding citizens, but will have little (if any) impact on either terrorists or criminals. This legislation is typical of surveillance hawks.

The underlying principle that is always deliberately avoided by surveillance hawks is that if one is looking for a needle in a haystack (trying to spot a terrorist in the larger general population), adding more hay (casting a wide net that spies on everyone) is not the way to find the needle. It is enough to make a reasonable person think the needle is not the object, after all.

Furthermore, since Australia is one of the Five Eyes nations (along with New Zealand, the United Kingdom, Canada, and the United States), the anti-encryption legislation will likely spread like a virus, infecting those other nations.

And since the vast majority of the technology companies providing devices and services to the Land Down Under are not Australian companies, the underlying vulnerabilities will be available for all of those devices and services — regardless of where (and by whom) they are used. Surveillance hawks have long claimed to seek some type of "single-use" or "safe" backdoor. Tech experts and companies have always replied with the simple fact that there is no such thing.

The Australian legislature goes to ridiculous lengths to make this law appear to differentiate between weakening the protection afforded to everyone on the one hand and creating a "safe" backdoor that is to be used only against terrorists and criminals. A draft of the legislation attempted to explain that alleged distinction:

> Systemic vulnerability means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.
>
> Systemic weakness means a weakness that affects a whole class of technology, but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.

The draft then goes on to explain how that supposedly differs from using those vulnerabilities and weaknesses on "target technology" that is "used, or is likely to be used, (whether directly or indirectly) by a particular person."

This "explanation" prompts a few reasonable questions:

• How, exactly, does one indirectly use a device or service?

• What about the fact that many devices and services are used by multiple users?

• What is the legal standard for backdooring the device or service of Person A simply because it is "likely to be used" by Person B?

The honest answers to these questions reveal the salient fact that that what the new law accomplishes is the defeat of commercially available encryption used by millions to protect their privacy and liberty. The end result is blanket — not targeted — surveillance.

Aside from the infantile notion that putting spyware on devices simply because they are "likely to be used, (whether directly or indirectly) by a particular person" is anything other than blanket surveillance, the warning of tech companies and experts should be heeded. That warning is that any backdoor creates a vulnerability that can be exploited by hackers — government or otherwise — against anyone using those devices and services. Period.

In this particular case, that warning was renewed — and ignored. As AFP News reported: "Global communications firms, including Google and Twitter, have repeatedly said the legislation would force them to create vulnerabilities in their products, such as by decrypting messages on apps, which could then by exploited by bad actors."

And since it is the devices and services offered by those global communications firms — along with global device manufacturers — that are targeted by this new law, the "bad actors" will have the ability to compromise devices around the world.

Considering that encryption serves as a fundamental part of protecting privacy and liberty in the digital age, this law can only be seen as a broadside attack on the rights of law-abiding citizens. For a government — which should place the protection of life, liberty, and property above all else — to attack encryption and risk opening millions around the world up to having their data and communications compromised simply to satisfy its own greed for access to more and more of the data of private citizens is inexcusable.